IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

REBECCA BROWN, *et al.*,

Plaintiffs,

v.

TRANSPORTATION SECURITY ADMINISTRATION, *et al.*,

Defendants.

Civil Action No. 2:20-cv-64-LPL

PROTECTIVE ORDER GOVERNING ACCESS TO, HANDLING OF, AND DISPOSITION OF POTENTIAL SENSITIVE SECURITY INFORMATION

In accordance with Section 525(d) of the Department of Homeland Security Appropriations Act, 2007, Public Law No. 109-295, § 525(d), 120 Stat. 1382, 1355 (Oct. 4, 2006), as reenacted (the "Act"), the Court hereby enters this Protective Order Governing Access to, Handling of, and Disposition of Potential Sensitive Security Information (the "Order") exchanged in the above-captioned matter (this "Litigation").

1. Scope

1.1 This Order shall govern any Document, information or other material that potentially contains "Sensitive Security Information" as defined herein, including Documents potentially containing Sensitive Security Information that are produced by the Parties, Documents produced by non-parties, and Documents produced by government agencies.

1.2 Nothing contained herein alters or affects in any manner a covered person's obligations and duties as set forth in 49 C.F.R. Part 1520.

2. Definitions

2.1 Cleared Counsel. The term "Cleared Counsel" shall refer to the attorneys and paralegal representing the Plaintiffs in this Litigation, who are not otherwise authorized to have

access to Sensitive Security Information pursuant to 49 C.F.R. Part 1520, but who TSA has cleared for access to specific Sensitive Security Information after determining that such access does not present a risk of harm to the nation based upon a criminal history records check, terrorist threat assessment, and evaluation of the sensitivity of the information as mandated by Section 525(d) of the Act. Cleared Counsel must agree to be bound by the terms of this protective order by signing attached EXHIBIT A.

2.2 Covered Person. The term "Covered Person" shall refer to any person who is authorized to have access to specific Sensitive Security Information pursuant to 49 C.F.R § 1520.7 and 1520.11, independent of this Litigation.

2.3 Documents. The term "Documents" shall include, but is not limited to, all written or printed matter of any kind, formal or informal, including originals, conforming and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise). The term further includes, but is not limited to, the following:

a. papers, correspondence, memoranda, notes, letters, reports, summaries, photographs, maps, charts, graphs, inter-office and intra-office communications, notations of any sort concerning conversations, meetings, or other communications, bulletins, teletypes, telegrams, telefacsimiles, invoices, worksheets, transcripts of any kind (including depositions and Court proceedings), legal briefs, pleadings and papers (including those filed with the Court) and drafts, alterations, modifications, changes and amendments of any kind to the foregoing;

b. graphic or oral records or representations of any kind, including, but not limited to, photographs, charts, graphs, microfiche, microfilm, videotapes, sound recordings of any kind, and motion pictures;

c. electronic, mechanical or electric records of any kind, including, but not limited to, tapes, cassettes, disks, recordings, electronic mail, films, typewriter ribbons, word processing or other computer tapes or disks, and all manner of electronic data processing storage.

2.4 Restricted Use Document. The term "Restricted Use Document" shall refer to any Document that contains Sensitive Security Information.

2.5 Parties. The terms "Party" and "Parties" refer to the parties to this Litigation and their counsel as well as any and all future parties to this Litigation.

2.6 Sensitive Security Information. The term "Sensitive Security Information" shall have the meaning set forth in 49 U.S.C. § 114(r)(1)(C), 49 C.F.R. § 1520.1 et seq., and as designated in orders issued by TSA pursuant to 49 U.S.C. § 114(r).

3. Identification and Review of Sensitive Security Information

3.1 All Documents sought to be produced or otherwise exchanged in connection with this Litigation that contain, or that the producing party has reason to believe contain, Sensitive Security Information, shall first be submitted to TSA for review, with an accompanying index of the submitted Documents, as required under 49 C.F.R. § 1520.9(a)(3).

3.2 TSA shall promptly complete a review to determine if any particular Document submitted contains Sensitive Security Information. Upon completion of this review, to the extent that a Document does not contain Sensitive Security Information, TSA shall authorize the release of the Document and the Document shall no longer be subject to this Order. Information that TSA has determined does not constitute Sensitive Security Information may be used and disclosed in any manner consistent with the disclosure procedures governing non-Restricted Use Documents exchanged in this Litigation.

3.3 Upon completion of this review, to the extent that TSA determines that a Document does contain Sensitive Security Information, the Document may only be produced to

Cleared Counsel in unredacted form pursuant to the terms of Sections 4.3 and 4.4. At a Party's request, such as when necessary to prepare or support a document for public filing, a Party may request that TSA redact the specific Sensitive Security Information from the face of the Document and provide such redacted version to the entity that submitted the Document for review. TSA shall authorize the production of such Documents as redacted and such redacted Documents may be used and disclosed in any manner consistent with the disclosure of non-Restricted Use Documents exchanged in this Litigation.

3.4 Should it come to TSA's attention that it may have inadvertently failed to designate material as Sensitive Security Information, TSA may review any Document to reassess whether it contains any Sensitive Security Information. To the extent that TSA determines upon re-review that the Document does not contain any Sensitive Security Information, TSA shall authorize the Document for production pursuant to Section 3.2. of this Order; to the extent TSA determines upon re-review that the Document does contain Sensitive Security Information, TSA shall apply the procedures of Section 3.3. of this Order and require that any Cleared Counsel or Covered Person immediately submit written certification to TSA that all copies of the Document have been destroyed.

4. Access to Sensitive Security Information

4.1 Access to the Sensitive Security Information under the terms and conditions of this Order shall be restricted to:

a. Covered Persons;

b. Cleared Counsel in accordance with Section 4.2 of this Order; and

c. Designated court reporters who have signed EXHIBIT A.

4.2 If Cleared Counsel seeks access to the Sensitive Security Information contained in any Restricted Use Document, Cleared Counsel must make a showing to TSA that they: (a) have

a substantial need for relevant Sensitive Security Information in the preparation of this case, and, (b) are unable without undue hardship to obtain the substantial equivalent of the relevant Sensitive Security Information by other means. If TSA determines that the Cleared Counsel seeking access has successfully made such showings, TSA will grant Cleared Counsel access to the specific Sensitive Security Information if TSA determines that such access would not present a risk of harm to the nation.

4.3 If TSA determines that it is appropriate to grant Cleared Counsel access to specific Sensitive Security Information pursuant to Section 4.2 of this Order, it will authorize production to the requesting Cleared Counsel of a Restricted Use Document with the specific Sensitive Security Information unredacted.

4.4 To the extent that a Restricted Use Document contains a range of Sensitive Security Information, some of which TSA determines is appropriate for production to Cleared Counsel and some of which is inappropriate for production under the criteria set forth in Section 4.2 of this Order and Section 525(d) of the Act, TSA shall redact the Sensitive Security Information that is inappropriate for production. TSA shall then authorize the production of such Restricted Use Document to Cleared Counsel only in such redacted form.

4.5 Should Cleared Counsel cease representing the Plaintiffs in this Litigation, for whatever reason, such Cleared Counsel shall no longer be cleared for access to Sensitive Security Information. Plaintiffs may elect to have a new attorney undergo the vetting process described in Section 525(d) of the Act in order to obtain access to Sensitive Security Information in this Litigation.

4.6 In the event that Cleared Counsel loses or relinquishes his or her clearance for access to Sensitive Security Information, for whatever reason, the former Cleared Counsel must promptly certify in writing to TSA that all Sensitive Security Information in his or her custody

has been destroyed or that all Sensitive Security Information in his or her custody has been transferred to the new Cleared Counsel in this Litigation.

4.7 All Restricted Use Documents subject to this Order in the possession Cleared Counsel, employees of Cleared Counsel, and party-designated consultants and experts shall be certified in writing to have been destroyed within 60 days of termination of this Litigation, including any appellate proceedings.

5. Non-Disclosure of Sensitive Security Information

5.1 Except as provided in this Order, persons authorized to have access to Sensitive Security Information pursuant to 4.1 of this Order are prohibited from disclosing, in any manner, or otherwise providing access to, Sensitive Security Information, however obtained, to any individual or entity.

5.2 Except as provided in this Order, persons authorized to have access to Sensitive Security Information pursuant to Section 4.1 of this Order are prohibited from aiding or assisting any person or entity in disclosing, in any manner, or otherwise providing access to, Sensitive Security Information.

5.3 Litigation support staff, including paralegals and administrative assistants, and expert consultants and witnesses may not be granted access to Sensitive Security Information unless authorized by TSA in writing.

5.4 Any authorized disclosure of Sensitive Security Information must be made pursuant to Sections 6, 7, and 8.

6. Production of Documents

6.1 Prior to production, the entity responsible for producing Restricted Use Documents shall label or stamp any such Document with the following language:

SUBJECT TO SENSITIVE SECURITY INFORMATION PROTECTIVE ORDER IN BROWN V. TSA, CIVIL ACTION NO. 2:20-cv-64-LPL (WESTERN DISTRICT OF PENNSYLVANIA)

SENSITIVE SECURITY INFORMATION WARNING: THIS RECORD MAY CONTAIN SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A 'NEED TO KNOW,' AS DEFINED IN 49 CFR PART 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTY OR OTHER ACTION.

6.2 All Restricted Use Documents shall be produced by creating password-protected adobe pdf files of the authorized Restricted Use Documents and sending them by means of either encrypted media (e.g., DVD or flash drive) or a secure file transfer system. The password must be provided by separate email.

6.3 Only persons authorized to have access to Sensitive Security Information pursuant to Section 4.1 of this Order may maintain custody of the media containing Restricted Use Document(s), and such persons have a duty to safeguard the media, the Restricted Use Document(s), and the Sensitive Security Information contained therein, from unauthorized disclosure. When not in the physical possession of such persons, the media containing the Restricted Use Document(s) shall be stored in a secured container, such as a locked desk or file cabinet.

6.4 Persons authorized to have access to Sensitive Security Information pursuant to Section 4.1 of this Order may create Documents containing Sensitive Security Information found in a Restricted Use Document, provided that any such Document is secured in the same or

equivalent manner, to the same or equivalent extent, and with the same restrictions on access as the media containing the Restricted Use Document as set forth in this Section 6.

7. Use of Sensitive Security Information in Depositions and Examinations

7.1 Sensitive Security Information that is authorized for production pursuant to Section 4 of this Order may be used and/or elicited during the deposition or examination of a witness, provided such witness is a Covered Person, subject to the following restrictions:

7.1.1 Only the individuals identified in Section 4.1 of this Order may be present in the room when such Sensitive Security Information is used and/or elicited.

7.1.2 To the extent that Cleared Counsel or a Covered Person wishes to use a Restricted Use Document as an exhibit at a deposition, the Cleared Counsel or Covered Person may print a limited number of hard copies of such Restricted Use Document using a secure printer located at the Cleared Counsel's or the Covered Person's place of employment for use solely as exhibits at the deposition, provided that at the conclusion of the deposition, the original marked deposition exhibit and all hard copies are collected and maintained by a court reporter authorized to have access to Sensitive Security Information in accordance with Section 4.1(c) of this Order. The court reporter shall secure the Restricted Use Documents in the same manner, to the same extent, and with the same restrictions on access prescribed in Section 6 of this Order.

7.1.3 Sensitive Security Information that is not authorized for release pursuant to Section 4 of this Order may not be used or elicited during the examination of a witness.

7.2 The court reporter who records a deposition shall promptly submit the deposition transcript to TSA for review. TSA shall promptly complete a review to determine if a deposition transcript contains Sensitive Security Information. To the extent that TSA determines, upon review of the deposition transcript, that the transcript contains Sensitive Security Information that is appropriate for release pursuant to Section 4 of this Order, TSA shall authorize the

transcript for release to counsel for Covered Persons and to Cleared Counsel with all such appropriate Sensitive Security Information unredacted from the transcript.

8. Use of Sensitive Security Information in Motions and Court Proceedings

8.1 No Party may file a Restricted Use Document or the Sensitive Security Information contained therein on the Court's public docket. A Party who wishes to use a Restricted Use Document or the Sensitive Security Information contained therein in connection with a motion or other submission to this Court must seek leave of court to file the Restricted Use Document and any pleadings, motions or other papers containing Sensitive Security Information under seal. *See* Standing Order 05-45 (Jan. 27, 2005). Where possible, only the portions of the filings that contain Sensitive Security Information shall be subject to a request to file under seal.

8.2 Sensitive Security Information shall not be disclosed in open court. If it becomes necessary to disclose Sensitive Security Information at a court hearing or trial, a Party must request leave of court to close to the public the portion of the proceeding discussing Sensitive Security Information.

9. Dispute Resolution

9.1 If a Party does not agree with TSA's determination that a Restricted Use Document contains Sensitive Security Information it shall request in writing that TSA issue a final order pursuant to 49 U.S.C. § 114(r) designating such information as Sensitive Security Information. TSA final orders concerning the designation of information as Sensitive Security Information are reviewable exclusively in the United States Court of Appeals in accordance with 49 U.S.C. § 46110.

9.2 To the extent there is a dispute concerning whether specific redacted or withheld Sensitive Security Information should be authorized for production under Section 4 of this Order

and Section 525(d) of the Act, the Parties shall meet and confer in an attempt to resolve the dispute consensually. For all unresolved disputes concerning whether specific Sensitive Security Information should be authorized for production, a Party (or Parties) may submit the dispute to the appropriate Court as identified below.

9.2.1 TSA final determinations concerning granting or denying access to specific Sensitive Security Information based upon relevance, substantial need, and the ability to obtain information without undue hardship, are reviewable by this Court. Any order by this Court granting access to Sensitive Security Information under this Section shall be immediately appealable to the United States Court of Appeals in accordance with Section 525(d) of the Act.

9.2.2 TSA final orders concerning whether a risk of harm to the nation is presented by granting access to specific Sensitive Security Information, either because of the sensitivity of the information or the results of the criminal history records check and terrorist threat assessment as set forth in Section 525(d) of the Act, are reviewable exclusively by the Court of Appeals in accordance with 49 U.S.C. § 46110.

10. Unauthorized Disclosures

10.1 If Sensitive Security Information is disclosed other than as authorized by this Order, the Party or person responsible for the unauthorized disclosure, and any other Party, person, firm or entity who is subject to this Order and learns of the unauthorized disclosure, shall immediately bring such disclosure to the attention of TSA.

10.2 The Party or person responsible for the unauthorized disclosure shall make every effort to obtain the return of the Sensitive Security Information (including, without limitation, from the person to whom the unauthorized disclosure was made and from any other person to whom Sensitive Security Information was transmitted as a direct or indirect result of the

unauthorized disclosure) and to prevent further disclosure on its own part or on the part of any person to whom the unauthorized disclosure was made.

10.3 In addition to any other remedies that are available under law, any Party, person, firm or entity responsible for an unauthorized disclosure of Sensitive Security Information protected by this Order may be subject to a civil penalty by TSA of up to $50,000, and all other remedies provided under 49 C.F.R. § 1520.17.

10.4 In the event that TSA determines that Cleared Counsel has intentionally, willfully or recklessly disclosed Sensitive Security Information in violation of this Order, TSA may, in the exercise of its sole discretion, revoke such Cleared Counsel's clearance for access to Sensitive Security Information. Furthermore, TSA may consider such intentional, willful or reckless disclosure in determining whether granting access to Sensitive Security Information to any member of a firm or entity that employed such Cleared Counsel, and/or to the Party whom that Cleared Counsel represents in this Litigation.

11. Reservation of Rights

11.1 In the event that TSA determines that a Document produced in this matter contains Sensitive Security Information and either (i) was not designated a Restricted Use Document or (ii) contains information inappropriate for production under the criteria set forth in Section 4.2 of this Order and Section 525(d) of the Act, TSA reserves the right to take any measures necessary to protect the Sensitive Security Information at issue, including designating the Document a Restricted Use Document or requiring Cleared Counsel to destroy all Documents containing the Sensitive Security Information that was inappropriate for production.

11.2 TSA reserves the right to revoke a Cleared Counsel's clearance in the event TSA obtains information that leads TSA to determine that granting such Cleared Counsel access to Sensitive Security Information presents a risk of harm to the nation.

11.3. If it comes to TSA's attention that information or items that it designated as Sensitive Security Information do not qualify as Sensitive Security Information or have ceased to qualify as Sensitive Security Information, TSA will promptly notify all Parties that it is withdrawing its Sensitive Security Information designation.

11.4 This Order is without prejudice to the rights of any Party or government agency to make any claim of privilege or to make any objection to discovery or use of Sensitive Security Information, or documents that may contain Sensitive Security Information, permitted by the Federal Rules of Civil Procedure, or any other statute, regulation, or authority.

SO ORDERED.

Dated: 2/9/22

Lisa Pupo Lenihan
U.S. Magistrate Judge

EXHIBIT A

Agreement to Abide by the Terms of the Protective Order Governing Access to, Handling of, and Disposition of Potential Sensitive Security Information in the matter of *Brown v. TSA*, No. 2:20-cv-64-LPL (W.D. Pa.)

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of SSI information as set forth in the Protective Order Governing Access to, Handling of, and Disposition of Potential Sensitive Security Information in the matter of *Brown v. TSA*, No. 2:20-cv-64-LPL (W.D. Pa.).

I make this Agreement in good faith, without mental reservation or purpose of evasion.

_____
Print Name

_____
Address

_____
Telephone Number

_____
Signature

WITNESS:

_____
Print Name

_____
Address

_____
Telephone Number

_____
Signature